CLAIMS:

1. A method of providing data integrity authentication and data protection, in which a set of data fragments is protected by a signature characterized in that
each data fragment of the set comprises its own unique identifier,
the signature comprises references to the respective unique identifiers of the data fragments of the set.

2. The method according to claim 1, in which the set is protected by multiple signatures, and in which the multiple signatures can originate from different sources.

3. The method according to claim 1, in which for each data fragment a hash is generated and the hashes of the data fragments of the set are used to compute the signature.

4. The method according to claim 1, in which the data fragments are expressed in XML.

5. The method according to claim 1, in which the data fragments constitute TV-Anytime metadata.

6. The method according to claim 1, in which the signature is stored according to the xmldsig standard.

7. The method according to claim 1, in which the set of data fragments is defined by a transform function on a superset of data fragments.

8. The method according to claim 1, in which a cannolization function is used before generating the signature.

9. The method according to claim 1, in which the references are also protected by the signature.

10. The method according to claim 1, in which at least one signature index file is added.

11. The method according to claim 1, in which the unique identifier in a particular data fragment starts with a unique identification of an organization that generated the particular data fragment.

12. The method according to claim 11, in which the unique identification is the DNS name of the organization.

13. The method according to claim 1, in which the reference is accompanied by a location indicator that indicates the location of the data fragment the reference refers to.

14. The method according to claim 13, in which the location indicator indicates the path through the data to the referenced data fragment.

15. The method according to claim 4, in which the signature is included in an XML document.

16. The method according to claim 4, in which the signature is provided in a wrapper XML document, comprising the original XML data document.

17. The method according to claim 4, in which the signature is provided in a separate XML document, referring to the original XML data document.

18. System (20) for providing data integrity authentication and data protection,

the system being arranged to receive and handle data fragments, of which a set of data fragments can be protected by a signature, characterized in that

the system comprises means to receive and handle data fragments of the set, each data fragment identified by a unique identifier,

the system further comprises at least one of

means for associating a signature with the protected data fragments of the set using their unique identifiers,

means for verifying a signature associated with the set using the unique identifiers of the protected data fragments, and

means for generating a signature that references the protected data fragments by their unique identifiers.

19. Signature device (13-15) for providing data integrity authentication and data protection,

the device being arranged to handle data fragments,

the device being arranged to generate a signature to protect a set of data fragments, characterized in that

the device is arranged to address each data fragment to be protected by a unique identifier included in the data fragment, and

the device is arranged to generate signature information comprising the unique identifiers to refer to the data fragments of the set.

20. Verification device (10) for verifying data integrity authentication and data protection,

the device being arranged to handle data fragments,

the device being arranged to verify a signature to protect a set of data fragments, characterized in that

the device is arranged to address each data fragment to be protected by a unique identifier included in the data fragment, and

the device is arranged to verify signature information comprising the unique identifiers to refer to the data fragments of the set.

21. Signal (11) comprising data fragments, of which a set of data fragments is protected by a signature, characterized in that

each data fragment of the set comprises its own unique identifier, and

the signature comprises references to the unique identifiers of the data fragments of the set.

22. Computer program product (12) for implementing the method of claim 1.